Remainder Theorem

Starting with: The Basics of Remainder

Before dwelling into 'RT', it's essential to be aware of some basics about remainder.
Consider N = DQ + R, where D is non-zero, Q and R are integers and $0 \leq R < D$.
In the foregoing equation; N is dividend, D is divisor, Q is quotient and R is the remainder. When R is zero, we say that the number (N) is completely divisible by D.

Ground Rules:

The following three ground rules shall be essential weapons of your armory while confronting Remainder questions in the future.

1. ***Remainder [(a x b) / c] = Remainder [a / c] x Remainder [b / c]***
2. ***Remainder [(a + b) / c] = Remainder [a / c] + Remainder [b / c]***
3. ***Remainder [(a – b) / c] = Remainder [a / c] – Remainder [b / c]***

Prime Numbers: The prime question

Before we get to business end of this article, it's essential that we talk about prime numbers since all the theorems are derived from prime numbers and its concepts in some way.
Prime numbers are all those numbers which are divisible only by 1 and itself. There are infinite prime numbers and they do not follow a fixed rule or Pattern of Occurrence. To this day, mathematicians have made multiple futile attempts to arrive at a single formula to represent all the prime numbers.
As we go along you will find many tit-bit's about primes (Hereinafter referred to as "TB").

Let us start with the Remainder Theorems

Four important remainders theorems are:

- ***Euler's theorem***
- ***Fermat little theorem***
- ***Wilson theorem***
- ***Chinese 'RT'***

1) Euler's theorem

Euler's theorem states that if p and n are coprime positive integers, then ———> $P^{\Phi(n)} = 1$ (mod n), where Φ(n)=n (1-1/a) (1-1/b)….

Before we move any further, let us understand what mod is. Mod is a way of expressing remainder of a number when it is divided by another number. Here φ (n) (Euler's totient) is defined as all positive integers less than or equal to n that are coprime to n. ***(Co-prime numbers are those numbers that do not have any factor in common.)***

For example ———> $24=2^3 \times 3$

———> Therefore, we get 24 x (1-1/2) (1-1/3) = 8

———> which means that there are 8 numbers co-prime to 24.

They are 1, 5, 7, 11, 13, 17, 19, 23.

Let us understand this theorem with an example:

Q.1) – Find the remainder of (7^100) / 66

Answer-

As you can see, 7 and 66 are co-prime to each other.

Therefore, ***Φ 66 = 66 x (1-1/2) x (1-1/3) x (1-1/11) = 20***

So, (7^100) = 1(mod 66)

TB – Mathematicians have been very keen to arrive at a formula which gives some prime numbers, Here is one of them. f (n) = n^2- n+1 for n = 2, 3,….. 40, but f (41) is composite.

2) Fermat little theorem

Fermat's theorem is an extension of Euler's theorem. If, in the above theorem, n is a prime number then,***p^{n-1} =1(mod n)***

Consider an example;

Q.2) Find remainder of 7^{41} is divided by 41.

Here, 41 is a prime number.

Therefore, **[7^{40} x 7 /41]** (By Fermat's theorem)

which is equal **to 7.**

TB – Wieferich prime*: is a prime number p such that p2 divides $2^{p-1} – 1$ relating with Fermat little theorem, Fermat's little theorem implies that if p > 2 is prime, then $2^{p-1} – 1$ is always divisible by p*

3) Wilson theorem

Wilson's theorem states that a number 'n' is prime ***if and only if*** **(n-1)! + 1 is divisible by n**

For example –

Q.3) Find the remainder when 30! Is divided by 31.

Here, 31 is a prime number.

From Wilson's theorem, we have **(31-1)! /31 = – 1**

Hence, 30 is the remainder. ***[whenever there is a negative remainder, subtract it from the divisor and you get the remainder]***

Let us have a look another example.

Q.4) Find the remainder when 29! Is divided by 31.

You can write **29!/31** as **———> 30 x 29! / 30 x 31 (multiplying numerator and denominator by 30)**

Therefore, 30! / 30 x 31 = 1

We have already found from Wilson theorem 30! /31 is 30. 30 in the denominator cancels out, hence the remainder is 1.

From the foregoing examples, the derivative arrived at from this theorem is, (P-2)! = 1(mod P)

4) Chinese Remainder Theorem

Let's understand this theorem with an example:

Q.5) – Rahul has certain number of cricket balls with him. If he divides them into 4 equal groups, 2 are left over. If he divides them into 7 equal groups, 6 are left over. If he divides them into 9 equal groups, 7 are left over. What is the smallest number of cricket balls could Rahul have?

Let N be the number of cricket balls.

N = 2(mod4) ————> equation 1

N = 6(mod7) ————> equation 2 &

N = 7(mod9) ————> equation 3.

From N=2(mod4) we get, N=4a+2

Substituting this in equation 2, we get the following equation:

4a + 2 = 6(mod7)

Therefore, 4a = 4(mod7)

Hence, 2 x 4a = 2 x 4(mod7)

This gives us a = 1(mod7)

Hence a = 7b+1.

Plugging this back to N=4a+2, we get….

N = 28b + 6

Substituting this to equation 2;

28b + 6 = 7(mod9)

28b = 1(mod9)

Therefore, b=1(mod9)

Hence b = 9c + 1.

Substituting this back to equation N=28b+6;

N = 28(9c+1) + 6

N = 252c + 34

The smallest positive value of N is obtained by setting c=0.

It gives us N = 34

TB – All prime numbers greater than 3 can be expressed as 6K+1 or 6K-1, this is another important result. You would be using this result a lot when it comes to number system problems.

Other Useful Concepts-

1) Chicken McNugget Theorem

Yes, these Chicken McNuggets have a theorem on their name. What do you have?

Q.6) In a certain game, the only points one can score is either 7or 9. What is the highest number one cannot obtain in this game?

This problem involves the application of Chicken McNugget Theorem. The theorem says the largest residue one can ever obtain from positive integers 'p' and 'q' is given by **(pq – p – q).**

So the highest number is **[(7 x 9) - 7 - 9] = 47.**

2) Concept of Cyclicity

Q.7) If n is a positive integer, what is the remainder when [$7^{(8n+3)}$ + 2] is divided by 5?

This problem can be easily solved with concept of cyclicity.

You should realize that unit digit of all numbers raised to powers start repeating itself.

For example, the cyclicity of 7 is 4. This means that the unit digits repeat after on every 4th power. See for yourself below:

$7^1 = 7$	$7^5 = 7$	$7^9 = 7$
$4^2 = 9$	$7^6 = 9$	$7^{10} = 9$
$7^3 = 3$	$7^7 = 3$	$7^{11} = 3$
$7^4 = 1$	$7^8 = 1$	

In this question, consider n=1.

You are looking at unit digit of 7^11 which will be 3 from concept of cyclicity.

Add two to it.

Therefore, last digit will be 5 for [$7^{(8n+3)}$ + 2]. Hence it's completely divisible by 5.

3) Concept of negative remainder

Remainder can never be negative; its minimum value can only be 0.

Consider an example of -30 / 7. Here, remainder is 5.

It would not be (-28 – 2 / 7), but [(-35+5)/7]

When you divide, you will get remainder of -2. Since remainder can never be negative, we subtract it from quotient, here 7 – 2 = 5.

Negative remainder is useful when you are trying to solve a problem with higher power.

Consider an example…….

Q.8) Find the remainder for 7^7^7 is divided 32

32 can be factored into 8 and 4,

Therefore, we will divide the question into two parts:

Remainder [7^7^7/8] x Remainder [7^7^7/4]

which gives: Remainder [(-1) ^7^7/8] x Remainder [3^7^7/4] [(-1) raised to odd power is -1 and raised to even power is 1]

Remainder [(-1)/8] x Remainder [(-1)/4]…. which gives

———> 7 x 3 = 21